

CONTENTS

SECTION I: HISTORY OF CRYPTOGRAPHY

1. **The Contribution of E.B. Fleissner and A. Figl for today's Cryptography**
O.J. HORAK 3
2. **On the History of Cryptography during WW2, and possible new Directions for Cryptographic Research**
T. TEDRICK 18

SECTION II: PUBLIC KEY CRYPTOGRAPHY

3. **Efficient Factoring based on Partial Information**
R.L.RIVEST, A. SHAMIR 31
4. **A Public-Key Cryptosystem based on Shift Register Sequences**
H. NIEDERREITER 35
5. **A Comment on Niederreiter's Public Key Cryptosystem**
B. SMEETS 40
6. **Implementation Study of Public Key Cryptographic Protection in an Existing Electronic Mail and Document Handling System**
J. VANDEWALLE, R. GOVAERTS, W. De BECKER, M. DECROOS, G. SPEYBROUCK 43
7. **Cryptanalysis of the Dickson-Scheme**
W.B. MÜLLER, R. NÖBAUER 50
8. **Simultaneous Security of Bits in the Discrete Log**
R. PERALTA 62
9. **On Public-Key Cryptosystems built using Polynomial Rings**
J.P. PIEPRZYK 73

SECTION III: SECRET KEY CRYPTOGRAPHY

10.	Is the Data Encryption Standard a Group? B.S. KALISKI, Jr., R.L. RIVEST, A.T. SHERMAN	81
11.	Two New Secret Key Cryptosystems H. MEIJER, S. AKL	96
12.	Cryptanalysts Representation of Nonlinearly filtered ML-Sequences T. SIEGENTHALER	103
13.	Authorized Writing for "Write-Once" Memories Ph. GODLEWSKI, G.D. COHEN	111

SECTION IV: SHIFTREGISTER SEQUENCES AND RELATED TOPICS

14.	On Functions of Linear Shift Register Sequences T. HERLESTAM	119
15.	On Feedforward Transforms and p-Fold Periodic p-Arrays Dong-sheng CHEN, Zong-duo DAI	130
16.	Generalized Multiplexed Sequences Mu-lan LIU, Zhe-xian WAN	135
17.	A Note on Sequences Generated by Clock Controlled Shift Registers B. SMEETS	142
18.	Using Algorithms as Keys in Stream Ciphers N.R. WAGNER, P.S. PUTTER, M.R. CAIN	149
19.	On the Linear Complexity of Combined Shift Register Sequences L. BRYNIELSSON	156
20.	Analysis of a Nonlinear Feedforward Logic for Binary Sequence Generators J. BERNASCONI, C.G. GÜNTHER	161
21.	Linear Complexity and Random Sequences R. A. RUEPPEL	167

SECTION V: CRYPTOGRAPHIC SYSTEMS AND APPLICATIONS

22.	Engineering Secure Information Systems D.W. DAVIES, W.L. PRICE	191
23.	The Chipcard - An Identification Card with Cryptographic Protection T. KRIVACHY	200
24.	Encryption: Needs, Requirements and Solutions in Banking Networks U. RIMENSBERGER	208
25.	The Role of Encipherment Services in Distributed Systems M.S. J. BAXTER, R.W. JONES	214
26.	Modeling of Encryption Techniques for Secrecy and Privacy in Multi-User Networks G.B. AGNEW	221
27.	Full Encryption in a Personal Computer System R. L. BRADEY, I.G. GRAHAM	231
28.	Showing Credentials without Identification Signatures transferred between unconditionally unlinkable Pseudonyms D. CHAUM	241
29.	Networks without User Observability - Design Options A. PFITZMANN, M. WAIDNER	245
30.	The verifiability of Two-Party Protocols R. V. BOOK, F. OTTO	254
31.	The Practice of Authentication G. J. SIMMONS	261
32.	Message Protection by Spread Spectrum Modulation in a Packet Voice Radio Link M. KOWATSCH, B.O. EICHINGER, F.J. SEIFERT	273
	Keywords	278
	Author Index	281